

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(use as many sheets as necessary)

Complete if Known

RECEIVED

Application Number	09/621,060
Filing Date	July 21, 2000 JUN 29 2001
First Named Inventor	Branstad
Group Art Unit	2785
Examiner Name	To be assigned Technology Center 2100
Attorney Docket Number	NTWK005/01/JS

Sheet 1 of 3

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	U.S. Patent Document Number Kind Code ² (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
6/24/01	A1	5,724,428	Rivest	03-03-98	380/37
6/22/05	A2	5,835,600	Rivest	11-10-98	380/44

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document Office ³ Number ⁴ Kind Code ⁵ (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
	B1					
	B2					

OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
M2	C1	M. BELLARE, R. CANETTI, and H. KRAWCZYK, "Keying Hash Functions for Message Authentication" in <i>Advances in Cryptology: Proceedings of CRYPTO '96</i> , LNCS 1109, N. Koblitz, ed., Springer-Verlag (1996), 1-15.	
M2	C2	R. CANETTI, J. GARAY, G. ITKIS, D. MICCIANCIO, M. NAOR, and B. PINKAS, "Multicast Security: A Taxonomy and Efficient Constructions" in <i>INFOCOM '99 Proceedings</i> , March 1999.	
M2	C3	P. ROGAWAY, "Design and Analysis of Message Authentication Codes," presented at the 1996 RSA Data Security Conference, January 19, 1996.	
M2	C4	P. ROGAWAY, "Bucket Hashing and its Application to Fast Message Authentication", <i>J. of Cryptology</i> , October 13, 1997.	
M2	C5	J. TOUCH, "Performance Analysis of MD5," proceedings of Sigcomm '95, Boston, MA.	
M2	C6	Atomic-2 Fast Security, http://www.isi.edu/atomic2/security/ , printed January 15, 2001.	
M2	C7	Cryptographic Technologies Adaptive Cryptographically Synchronized Authentication (ACSA), http://www.pgo.com/research/nailabs/cryptographic/adaptive-cryptographic.asp , printed January 12, 2001.	
M2	C8	D. Balenson, et al., ACSA Kickoff Brief presented to DARPA on September 11, 1998.	
M2	C9	D. Balenson, et al., ACSA Presentation to the DARPA/ITO Next Generation Internet (NGI) Principal Investigator's (PI) Meeting held on October 29, 1998.	
M2	C10	D. Balenson, et al., ACSA Presentation to the XIWT Workshop on Information Assurance and Trustworthy Networks held November 18, 1998.	
M2	C11	D. Carman, "Adaptively Trading Off Strength and Performance in Network Authentication," Presentation at the RSA Conference 2000 held January 19, 2000.	
M2	C12	D. Balenson, et al., ACSA Model and Analysis Document - Revision 1.0 delivered to DARPA on December 7, 1998, TIS Report #0758	
M2	C13	D. Carman, et al., ACSA Prototype System Design Document, Revision 1.0, May 12, 1999, TIS Report #0764	

¹ See attached Kinds of U.S. Patent Documents.² Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3).³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible.⁵ Applicant is to place a check mark here if English language Translation is attached.